Europ. J. Combinatorics (1999) **20**, 279–292
Article No. eujc.1998.0291
Available online at http://www.idealibrary.com on IDEAL®

On the Isomorphism Problem for Finite Cayley Graphs of Bounded Valency

CAI HENG LI AND CHERYL E. PRAEGER

For a subset S of a group G such that $1 \notin S$ and $S = S^{-1}$, the associated Cayley graph $\mathrm{Cay}(G, S)$ is the graph with vertex set G such that $\{x, y\}$ is an edge if and only if $yx^{-1} \in S$. Each $\sigma \in \mathrm{Aut}(G)$ induces an isomorphism from $\mathrm{Cay}(G, S)$ to the Cayley graph $\mathrm{Cay}(G, S^\sigma)$. For a positive integer m, the group G is called an m-CI-group if, for all Cayley subsets S of size at most m, whenever $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ there is an element $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$. It is shown that if G is an m-CI-group for some $m \geq 4$, then $G = U \times V$, where $(|U|, |V|) = 1$, U is abelian, and V belongs to an explicitly determined list of groups. Moreover, Sylow subgroups of such groups satisfy some very restrictive conditions. This classification yields, as corollaries, improvements of results of Babai and Frankl. We note that our classification relies on the finite simple group classification.

1. INTRODUCTION

This paper is a contribution to the study of isomorphisms between Cayley graphs for a finite group G. Automorphisms of the group G induce isomorphisms of Cayley graphs for G in a natural way, and for some groups G, whenever two Cayley graphs for G are isomorphic there is an isomorphism between them which is induced by an automorphism of G. If the latter property is true for all Cayley graphs of G of valency at most m (for a positive integer m), then the group G is called an m-CI-*group*. In this paper we give a classification of finite m-CI-groups for $m \geq 4$. Further, we derive, as corollaries of this classification, improvements of several results of Babai and Frankl [4, 5]. We also derive strong restrictions on the Sylow subgroups of m-CI-groups for $m \geq 2$.

Let G be a finite group. A subset S of G is called a *Cayley subset* if $1_G \notin S$ and $S = S^{-1} := \{s^{-1} \mid s \in S\}$, and the *Cayley graph* of G with respect to S is the graph $\mathrm{Cay}(G, S)$ with vertex set G and with x and y adjacent if and only if $yx^{-1} \in S$. Each element $\sigma \in \mathrm{Aut}(G)$ induces an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, S^\sigma)$, and $\mathrm{Cay}(G, S)$ is called a *CI-graph* of G if, whenever $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, there is an element $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$ (CI stands for *Cayley Isomorphism*). Note that $\mathrm{Cay}(G, S)$ is a regular graph of *valency* $|S|$. Thus G is an m-CI-group if all Cayley graphs for G of valency at most m are CI-graphs, and further we say that a finite group G is a *CI-group* if G is a $|G|$-CI-group.

The problem of determining CI-groups has received considerable attention in the literature. Interest in the problem stems from a conjecture of Adám [1] in 1967 that all finite cyclic groups are CI-groups. This conjecture was disproved by Elspas and Turner [9] shortly afterwards, when they showed that $\mathbb{Z}_{16}$ is not a CI-group. However, since then, a lot of work has been done to determine which cyclic groups are CI-groups (see for example [2, 18, 21]). The study of finite CI-groups in general began with a paper of Babai [3] in 1977. In 1978 Babai and Frankl [4] proved that if G is a CI-group of odd order, then either G is abelian or G has an abelian normal subgroup of index 3 and its Sylow 3-subgroup is elementary abelian, $\mathbb{Z}_9$ or $\mathbb{Z}_{27}$; they also showed in [5] that if G is a finite insoluble CI-group, then $G = L \times N$, where $(|L|, |N|) = 1$, $L \cong \mathrm{L}_2(5)$, $\mathrm{SL}_2(5)$, $\mathrm{L}_2(13)$ or $\mathrm{SL}_2(13)$, and N is a direct product of elementary abelian groups. Further results on elementary abelian CI-groups can be found in [8, 11, 13, 20].

0195-6698/99/040279 + 14 $30.00/0

TABLE 1.

r, s	e
$r = 0, s \geq 1$	3
$r \geq 1, s = 0$	2 or 4
$r \geq 1, s \geq 1$	6

In a different direction, in 1977 Toida [24] proved that all (undirected) Cayley graphs of valency 3 for cyclic groups are CI-graphs. This result and work of Babai suggested to Xu [26] in 1988 that it would be helpful to investigate finite m-CI-groups for small values of m. This was begun by Xu and others for abelian groups for $m \leq 5$ (see for example [7, 10, 12]). On the other hand, the authors showed in [15] that a finite nonabelian simple group G is a 2-CI-group if and only if G is A_5 or $L_2(8)$, and the only nonabelian simple 3-CI-group is A_5. The main aim of this paper is to classify m-CI-groups for $m \geq 4$ in the sense that an explicit list containing all such groups is given. As a corollary, we obtain a classification of CI-groups which is an improvement of the results of Babai and Frankl in [4, 5].

Two elements a, b of a group G are said to be *fused* if $a = b^\sigma$ for some $\sigma \in \mathrm{Aut}(G)$, and to be *inverse-fused* if $a = (b^{-1})^\sigma$ for some $\sigma \in \mathrm{Aut}(G)$. The only Cayley subsets of size 1 consist of a single involution (element of order 2), and hence G is a 1-CI-group if and only if all involutions of G (if any) are fused. It is clear that an m-CI-group is also a k-CI-group for each positive integer $k \leq m$, so it follows from the definition that if G is a 2-CI-group then any two elements of G of the same order are fused or inverse-fused (see Lemma 2.2). For convenience, we call a group with the latter property an *FIF-group* (FIF stands for fused or inverse-fused). In [15] we classified the finite nonabelian simple FIF-groups, and further in [16] we gave a good description of arbitrary finite FIF-groups. In the present paper we apply these results to obtain a classification of m-CI-groups with $m \geq 4$.

The notation and terminology used in this paper are standard (see for example [23, 25]). In particular, a direct product of cyclic groups of the same order is said to be *homocyclic*. For groups G and H, $G \rtimes H$ will denote an arbitrary semi-direct product of G by H. Let M be an abelian group all of whose Sylow subgroups are homocyclic, and let n be the exponent of M. We define certain nonabelian extensions of such homocyclic groups M. Let r, s be non-negative integers such that $r + s \geq 1$, and suppose that there exists an integer l such that $1 < l < n$ and l has *order e modulo n* (that is, e is the least positive integer such that $l^e \equiv 1 \pmod{n}$ and we write $o(l \bmod n) = e$) and in addition r, s, e are as in one of the lines of Table 1.

Then we define

$$H_e(M, 2^r 3^s, l) = M \rtimes \langle z \rangle = M \rtimes \mathbb{Z}_{2^r 3^s},$$

where $x^z = x^l$ for all $x \in M$. Note that the assumptions on l imply that no nontrivial Sylow subgroup of $\langle z \rangle$ centralizes M. The main result of this paper is the following.

THEOREM 1.1. *Let G be an m-CI-group for some $m \geq 4$. Then $G = U \times V$, where $(|U|, |V|) = 1$, U is abelian, and either $V = 1$ or V is one of the following:*

(i) Q_8, $\mathbb{Z}_3^2 \rtimes Q_8$, A_5, $SL_2(5)$;
(ii) $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_{3^s}$, $Q_8 \rtimes \mathbb{Z}_{3^s}$ *for some* $s \geq 1$;
(iii) $H_e(M, 2^r 3^s, l)$, *where M is abelian, r, s and e satisfy one of the lines of Table 1 and* $o(l \bmod n) = e$;
(iv) $Q_8 \times H_3(M', 3^s, l')$, $H_2(M, 2^r, l) \times H_3(M', 3^s, l')$, *where* 2, 3, $|M|$ *and* $|M'|$ *are pairwise coprime; M, M' are abelian, $r, s \geq 1$ and $l, l' > 1$.*

Further, let p be a prime dividing $|G|$ and let G_p be a Sylow p-subgroup of G. If $p > [\frac{m}{2}]$, then G_p is homocyclic; if $p = [\frac{m}{2}]$, then G_p is elementary abelian, cyclic or Q_8; if $p < [\frac{m}{2}]$, then either G_p is elementary abelian, or $G_p \cong \mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_9$ or Q_8.

It was proved in [14] that A_5 is not a 29-CI-group and $SL_2(5)$ is not a 58-CI-group. It therefore follows from Theorem 1.1 and [14] that all 58-CI-groups are soluble. In particular, neither A_5 nor $SL_2(5)$ is a CI-group. Taking $m = |G|$, Theorem 1.1 gives a classification of CI-groups which is an improvement of the results of [4, 5]. We must point out that, since the results of [15, 16] rely on the finite simple group classification, so also do the results of this paper.

COROLLARY 1.2. *Suppose that G is a CI-group. Then each Sylow subgroup of G is elementary abelian, or isomorphic to $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$ or Q_8. Moreover, $G = U \times V$, where $(|U|, |V|) = 1$, U is abelian, and either $V = 1$ or V is one of the following:*

(i) Q_8, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$, $Q_8 \rtimes \mathbb{Z}_3$, $Q_8 \rtimes \mathbb{Z}_9$, $\mathbb{Z}_3^2 \rtimes Q_8$;
(ii) $H_e(M, 2^r 3^s)$, *where M is abelian, r, s and e satisfy one of the lines of Table 1 and $o(l \bmod n) = e$;*
(iii) $Q_8 \times H_3(M', 3^s, l')$, $H_2(M, 2^r, l) \times H_3(M', 3^s, l')$, *where M, M' are abelian,* $1 \le r \le 3$, $1 \le s \le 2$ *and* $l, l' > 1$.

REMARK. (i) Nowitz [20] proved that $\mathbb{Z}_2^6$ is not a 31-CI-group. So not all of the groups listed in Theorem 1.1 are necessarily m-CI-groups for every value of m. It is difficult to determine precisely which groups listed in Theorem 1.1 are indeed m-CI-groups for a given $m \ge 4$. For example, for a prime p, it is not known whether $\mathbb{Z}_p^4$ is a CI-group, see [20, Question (1)] and [8]. It would be interesting to know whether $\mathbb{Z}_p^4$ was an m-CI-group for 'small' values of m.

PROBLEM 1.3. Determine which of the groups listed in Theorem 1.1 are m-CI-groups for certain small values of m.

In Section 2 we collect together several preliminary results which will be used later. Then in Section 3 we determine the possible structure of Sylow subgroups of m-CI-groups for $m \ge 2$. In Section 4 we use the results of [16] to obtain a good description of the structure of finite 2-CI-groups and investigate in more detail the structure of certain families of examples. We prove some technical lemmas in Section 5, and finally we prove Theorem 1.1 in Section 6.

2. PRELIMINARY RESULTS

We begin with some elementary observations about m-CI-groups. Let n be a positive integer. Then C_n denotes a cycle of size n, $K_{n,n}$ the complete bipartite graph of order $2n$, and for a graph Γ, $n\Gamma$ denotes a graph which consists of n vertex-disjoint copies of Γ. The first lemma is an immediate consequence of the definitions given in Section 1.

LEMMA 2.1. *Let G be a finite group.*

(1) *For any $S, T \subseteq G \setminus \{1\}$, $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ if and only if $\mathrm{Cay}(\langle S\rangle, S) \cong \mathrm{Cay}(\langle T\rangle, T)$.*
(2) *If G is an m-CI-group for some integer $m \ge 1$ and N is a characteristic subgroup of G, then N is also an m-CI-group.*

LEMMA 2.2. *If G is an m-CI-group for some $m \ge 2$, then any two elements of G of the same order are fused or inverse-fused under* $\mathrm{Aut}(G)$.

PROOF. Suppose that G is an m-CI-group for some $m \geq 2$. Since m-CI-groups are 1-CI-groups, all involutions of G are fused under $\mathrm{Aut}(G)$. Let $a, b \in G$ be such that $o(a) = o(b) > 2$. Then clearly $\mathrm{Cay}(G, \{a, a^{-1}\}) \cong \frac{|G|}{o(a)} C_{o(a)} \cong \mathrm{Cay}(G, \{b, b^{-1}\})$. Since G is a 2-CI-group, there exists $\alpha \in \mathrm{Aut}(G)$ such that $\{a, a^{-1}\}^\alpha = \{b, b^{-1}\}$, that is, $a^\alpha = b$ or b^{-1}. □

Next, we quote two results about FIF-groups from [16], the first quite elementary, but the second less so.

LEMMA 2.3. *Let G be an FIF-group, and let N be a characteristic subgroup of G.*

(i) ([16, Lemma 2.1]) *Both N and G/N are FIF-groups.*
(ii) ([16, Lemma 6.11 (ii)]) *Suppose that $N \cong \mathbb{Z}_p^d$ for some $d \geq 1$ and some prime p, that N is a minimal normal subgroup of G with $\mathbf{C}_G(N) = N$, and that $G \cong \mathbb{Z}_p^d \rtimes \mathbb{Z}_k$ for some $k > 1$. Then $\frac{1}{2}\varphi(k)$ divides d, where $\varphi(k)$ is the Euler phi-function (that is, the number of positive integers less than k and coprime to k).*

As usual a group G is said to be *indecomposable* if $G = A \times B$ implies that $A = 1$ or $B = 1$. In the following, we shall say that G is *coprime-indecomposable* if $G = A \times B$ such that $(|A|, |B|) = 1$ implies that $A = 1$ or $B = 1$. For a group G and a subgroup H of G, we shall denote by $H \ char \ G$ the fact that H is a characteristic subgroup of G.

3. SYLOW SUBGROUPS OF m-CI-GROUPS

In this section we give a description of Sylow subgroups of m-CI-groups for $m \geq 2$. First we consider Sylow 2-subgroups.

LEMMA 3.1. *Let G be an m-CI-group with $m \geq 2$ and let G_2 be a Sylow 2-subgroup of G. Then G_2 is elementary abelian, cyclic, or generalized quaternion. Further, if $m \geq 4$, then G_2 is elementary abelian, cyclic or Q_8; if $m \geq 6$, then G_2 is elementary abelian, $\mathbb{Z}_4$, $\mathbb{Z}_8$ or Q_8.*

PROOF. By [17, Theorem 1.3], G_2 is elementary abelian, cyclic, or generalized quaternion. Assume that $m \geq 4$ and that G_2 is generalized quaternion, that is,

$$G_2 = \langle x, y \mid x^{2^n} = 1,\ y^2 = x^{2^{n-1}},\ y^{-1}xy = x^{-1} \rangle.$$

Suppose that $n \geq 3$, and let $z = x^{2^{n-3}}$. Then $\langle z \rangle \cong \mathbb{Z}_8$ and $\langle y, z^2 \rangle \cong \mathrm{Q}_8$. Let $S = \{z, z^{-1}, z^3, z^{-3}\} (= \langle z \rangle \setminus \langle z^2 \rangle)$ and $T = \{z^2, z^{-2}, y, y^{-1}\} (= \langle y, z^2 \rangle \setminus \langle yz \rangle)$. Then $S = \mathbb{Z}_8 \setminus \mathbb{Z}_4$ and $T = \mathrm{Q}_8 \setminus \mathbb{Z}_4$. Thus it is easy to see that $\mathrm{Cay}(\langle S \rangle, S) \cong K_{4,4} \cong \mathrm{Cay}(\langle T \rangle, T)$ and so $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$. However, since $o(z) = 8$ and $o(z^2) = o(y) = 4$, S and T cannot be conjugate under $\mathrm{Aut}(G)$, which is a contradiction. Thus $n = 2$ and $G_2 = \mathrm{Q}_8$.

Assume that $m \geq 6$ and that G_2 is cyclic. Then by [13, Proposition 3.2(1)], $G_2 \cong \mathbb{Z}_2$, $\mathbb{Z}_4$ or $\mathbb{Z}_8$. □

Next we consider Sylow p-groups for odd primes p. For a positive integer k, a group G is said to have the *k-CI property* if all Cayley graphs of G of valency k are CI-graphs. Thus an m-CI-group has the k-CI property for all $k \leq m$. The following lemma draws together some elementary results from [16] and [17].

LEMMA 3.2. *Suppose that G is an m-CI-group for $m \geq 2$. Let p be an odd prime dividing $|G|$ and G_p a Sylow p-subgroup of G. Then G_p is homocyclic. Moreover,*

(i) *if* $p = \left[\frac{m}{2}\right]$, *then* G_p *is elementary abelian or cyclic;*

(ii) *if* $p < \left[\frac{m}{2}\right]$, *then* G_p *is elementary abelian or* $\mathbb{Z}_9$.

PROOF. By Lemma 2.2, G is an FIF-group, and so, by [16, Theorem 1.1], G_p is homocyclic. Further, by [17, Theorem 1.5], if $p = [\frac{m}{2}]$, then either G_p is of exponent p, or G_p is cyclic, so part (i) holds; if $p < [\frac{m}{2}]$, then either G_p is of exponent p, or G_p is both cyclic and of exponent 9, so part (ii) holds.

4. FINITE m-CI-GROUPS FOR $m \leq 3$

In this section we study m-CI-groups for $m \leq 3$. By the definition, a group G is a 1-CI-group if and only if all involutions of G are fused under $\mathrm{Aut}(G)$. So from now on we shall assume that $m \geq 2$. The simple m-CI-groups for $m = 2, 3$ are known.

THEOREM 4.1 ([16, THEOREM 1.3]). *Suppose that G is a nonabelian simple group. Then*

(i) *G is a 2-CI-group if and only if $G = \mathrm{A}_5$ or $\mathrm{L}_2(8)$,*
(ii) *G is a 3-CI-group if and only if $G = \mathrm{A}_5$.*

A classification of finite FIF-groups is given in [16], which, together with Lemma 3.1, provides a good description of finite 2-CI-groups.

THEOREM 4.2. *Suppose that G is a finite 2-CI-group. Then a Sylow p-subgroup G_p of G is either homocyclic, or $p = 2$ and G_2 is elementary abelian, cyclic or generalized quaternion. Moreover, $G = X_1 \times \cdots \times X_l$, where $(|X_i|, |X_j|) = 1$ and X_i is coprime-indecomposable, and one of the following holds:*

(1) *$X_i = M \rtimes \mathbb{Z}_n$, where $(|M|, n) = 1$, and M is nilpotent;*
(2) *$X_i = (L \times M) \rtimes ((H \rtimes K) \times \mathbb{Z}_n)$, where $|L|, |M|, |H|, |K|$ and n are pairwise coprime, and*
    (i) *$L \times M$ is nilpotent, and is maximal among the normal nilpotent Hall subgroups of X_i, $\langle M, H\rangle = M \times H$ and $\langle L, \mathbb{Z}_n\rangle = L \times \mathbb{Z}_n$,*
    (ii) *$H \rtimes K$ is indecomposable and noncyclic, neither H nor K centralizes a Sylow subgroup of L, and $(L, H \rtimes K)$ satisfies one of the lines in Table 2.*
(3) *$X_i = \mathrm{A}_5, \mathrm{L}_2(8), \mathrm{SL}_2(5), \mathrm{SL}_2(7)$ or $\mathrm{SL}_2(9)$.*

PROOF. By Lemmas 3.1 and 3.2, we have the conclusions about Sylow subgroups of G. By Lemma 2.2, any two elements of G of the same order are fused or inverse-fused, so G is a group on the list of [16, Theorem 1.1]. Thus $G = X_1 \times \cdots \times X_l$, where $(|X_i|, |X_j|) = 1$ and each X_i is coprime-indecomposable. Further, by Lemma 3.1, a Sylow 2-subgroup of a 2-CI-group is elementary abelian, cyclic or generalized quaternion. Therefore, if X_i is soluble, then we conclude from [16] that X_i is as in part (1) or (2); if X_i is insoluble, then it follows from [16] and the Atlas [6] that X_i is as in part (3). □

Next we prove several properties about the semidirect products occurring in Theorem 4.2, which will be used in the ensuing sections. First we consider the groups appearing in Theorem 4.2 (1).

TABLE 2.

L	$H \rtimes K$	conditions
$\mathbb{Z}_2^3$	$\mathbb{Z}_{7^t} \rtimes \mathbb{Z}_{3^s}$	$t, s \geq 1$
$\mathbb{Z}_{5^{u_1}7^{u_2}11^{u_3}}^2$	$\mathbb{Z}_{3^t} \rtimes \mathbb{Z}_{2^r}$	$r, t \geq 1, u_1 + u_2 + u_3 \geq 1$
$\mathbb{Z}_{3^{u_1}}^4 \times \mathbb{Z}_{19^{u_2}}^2$	$\mathbb{Z}_{5^t} \rtimes \mathbb{Z}_{2^r}$	$r, t \geq 1, u_1 + u_2 \geq 1$
$\mathbb{Z}_{7^{u_1}11^{u_2}19^{u_3}}^2$	$\mathbb{Z}_{3^{t_1}5^{t_2}} \rtimes \mathbb{Z}_{2^r}$	$r, t_1, t_2 \geq 1, u_1 + u_2 \geq 1, u_3 \geq 1,$ $[\mathbb{Z}_{19^{u_3}}, \mathbb{Z}_{3^{t_1}}] = 1, [\mathbb{Z}_{7^{u_1}11^{u_2}}^2, \mathbb{Z}_{5^{t_2}}] = 1$
$\mathbb{Z}_{3^{u_1}}^6 \times \mathbb{Z}_{19^{u_2}}^2$	$\mathbb{Z}_{7^{t_1}5^{t_2}} \rtimes \mathbb{Z}_{2^r}$	$r, t_1 \geq 1, u_1 + u_2 \geq 1, t_2 = 0 \Leftrightarrow u_2 = 0$ $[\mathbb{Z}_{3^{u_1}}^6, \mathbb{Z}_{5^{t_2}}] = 1, [\mathbb{Z}_{19^{u_2}}^2, \mathbb{Z}_{7^{t_1}}] = 1$
$\mathbb{Z}_{5^{u_1}11^{u_2}}^2$	$\mathbb{Z}_{3^{t_1}7^{t_2}} \rtimes \mathbb{Z}_{2^r}$	$u_1, t_1, t_2, r \geq 1, u_2 \geq 0, [\mathbb{Z}_{11^{u_2}}^2, \mathbb{Z}_{7^{t_2}}] = 1$
$\mathbb{Z}_q^2$	$Q_8 \rtimes \mathbb{Z}_{3^s}$	$q \neq 1$, *each prime divisor of* q *lies in* $\{3, 5, 7, 11, 23\}$, *and if* 3 *divides* q *then* $M = 1, s = 0$ *and* $n = 1$

LEMMA 4.3. *Let $G = M \rtimes \langle z \rangle$ be a 2-CI-group, where $(|M|, o(z)) = 1$ and M is nilpotent, and suppose that M has a Sylow p-subgroup $M_p = \mathbb{Z}_{p^s}^d$ for some prime p. Suppose further that $M_p \not\leq \mathbf{Z}(G)$, and let $g \in \langle z \rangle \setminus \mathbf{C}_{\langle z \rangle}(M_p)$. Then either*

(i) *$g^2 \notin \mathbf{C}_{\langle z \rangle}(M_p)$ and $\langle a \rangle \cap \langle a^g \rangle = 1$ for all $a \in M_p$, or*
(ii) *$p \geq 3$, and there exist positive integers e, l such that $e \in \{2, 3, 4, 6\}$, e divides $o(g)$, $1 < l < p^s$, $o(l \bmod p^s) = e$, and $g^{-1}ag = a^l$ for all $a \in M_p$; in particular, $g^e \in \mathbf{C}_{\langle z \rangle}(M_p)$.*

PROOF. Let $K = \langle M, g \rangle$. Since M is characteristic in G and $\langle g \rangle$ is characteristic in $\langle z \rangle$, it follows that K is characteristic in G, and so by Lemma 2.3, K is an FIF-group. Let e be the smallest positive integer such that $g^e \in \mathbf{C}_{\langle z \rangle}(M_p)$. Then e divides $o(g)$ and $(e, p) = 1$ (since $(o(g), p) = 1$).

First assume that g normalizes no nontrivial cyclic subgroups of M_p, that is, for all $x \in M_p \setminus \{1\}$, $x^g \notin \langle x \rangle$. Then it follows that $\langle x \rangle \cap \langle x^g \rangle = 1$ for all $x \in M_p$. If $g^2 \in \mathbf{C}_{\langle z \rangle}(M_p)$ then for some $x \in M_p \setminus \{1\}$, $x^{g^2} = x$ and so $(x \cdot x^g)^g = x^g \cdot x = x \cdot x^g$ and by our assumption on g we must therefore have $x \cdot x^g = 1$, that is $x^g = x^{-1}$, which is a contradiction. Thus $g^2 \notin \mathbf{C}_{\langle z \rangle}(M_p)$, and part (i) holds.

Now assume that g normalizes at least one nontrivial cyclic subgroup of M_p. Let p^t be the maximum of the orders of the cyclic subgroups of M_p which are normalized by g. Take $a \in M_p$ such that $o(a) = p^t$ and $a^g = a^l$ for some integer l with $1 \leq l < p^t$. Note that since $o(a^l) = o(a)$, $(l, p) = 1$. Further, $a^{l^e} = a^{g^e} = a$ and so $l^e \equiv 1 \pmod{p^t}$. We use the following steps to complete the proof of the lemma.

(1). *For each $x \in M_p$ with $o(x) = p^t$, $x^g = x^{i(x)}$ for some integer $i(x)$ with $1 \leq i(x) < p^t$.* Since $o(x) = o(a)$ and K is an FIF-group, there exists $\alpha \in \mathrm{Aut}(K)$ and $\varepsilon = \pm 1$ such that $a^\alpha = x^\varepsilon$. Since $K = M \rtimes \langle g \rangle$, $g^\alpha = cg^j$ where $c \in M \leq \mathbf{C}_K(M_p)$ and j is an integer coprime to $o(g)$. Therefore,

$$g^{-j}x^\varepsilon g^j = g^{-j}c^{-1}x^\varepsilon cg^j = (g^\alpha)^{-1}a^\alpha g^\alpha = (g^{-1}ag)^\alpha = (a^l)^\alpha = x^{l\varepsilon}.$$

Thus $g^{-j}xg^j = x^l$. Since $(j, o(g)) = 1$, we have $g^{-1}xg = x^{i(x)}$ for some integer $i(x)$ with $1 \le i(x) < p^t$.

(2). *For each $x \in M_p$ with $o(x) = p^t$, we have $i(x) = l$.* If M_p is cyclic, then clearly $i(x) = l$. Thus assume that M_p is not cyclic, so there exists $b \in M_p$ such that $o(b) = p^t$ and $\langle b\rangle \cap \langle a\rangle = 1$. Then $o(ab) = p^t$, and by step (1), $(ab)^g = (ab)^{i(ab)}$ for some integer $i(ab)$ such that $1 \le i(ab) < p^t$. So

$$a^l b^{i(b)} = a^g b^g = (ab)^g = (ab)^{i(ab)} = a^{i(ab)} b^{i(ab)},$$

and hence $a^{l-i(ab)} = b^{i(ab)-i(b)}$. Since $\langle a\rangle \cap \langle b\rangle = 1$, it follows that $i(b) = i(ab) = l$. Let $x \in M_p$ be an arbitrary element of order p^t. Then either $\langle x\rangle \cap \langle a\rangle = 1$ or $\langle x\rangle \cap \langle b\rangle = 1$. Thus by the previous argument, $i(x) = i(a)$ or $i(b)$, so $i(x) = l$.

(3). *$p^t = p^s$, and $o(l \bmod p^s) = e$.* It follows from step (2) that, for all $y \in M_p$ with $o(y) \le p^t$, $y^g = y^l$. Suppose that $p^t < p^s$. Take an element $b \in M_p$ with $o(b) = p^{t+1}$. By the maximality of t, $b^g \notin \langle b\rangle$. However, since $o(b^p) = p^t$, by step (2), $(b^p)^g = b^{lp}$. Thus $\langle b\rangle \cap \langle b^g\rangle = \langle b^p\rangle$, and so $\langle b, b^g\rangle \cong \mathbb{Z}_{p^{t+1}} \times \mathbb{Z}_p$. Hence $b^g = b^j c$ for some integer j and some $c \in M_p$ such that $o(c) = p$ and $\langle b\rangle \cap \langle c\rangle = 1$. Therefore, $b^{jp} = (b^j c)^p = (b^g)^p = (b^p)^g = b^{lp}$. Consequently, $jp \equiv lp \pmod{p^{t+1}}$, and so $j = kp^t + l$ for some integer k. Thus $b^g = b^j c = b^l b^{kp^t} c$. Let $c_0 = b^{kp^t} c$. Then $o(c_0) = p$, $\langle c_0\rangle \cap \langle b\rangle = 1$, $b^g = b^l c_0$ and $c_0^g = c_0^l$ (since $o(c_0) = p < p^{t+1}$). By induction on i, we have

$$b^{g^i} = b^{l^i} c_0^{i l^{i-1}}, \text{ for } i \ge 1.$$

Taking $i = e$, we have $c_0^{el^{e-1}} = b^{1-l^e}$ as $b^{g^e} = b$. Since $\langle c_0\rangle \cap \langle b\rangle = 1$, we have that $c_0^{el^{e-1}} = 1$ and so p divides el^{e-1}, contradicting the fact that $(el, p) = 1$. Therefore, $p^t = p^s$, and so for all $x \in M_p$, $x^g = x^l$. From the definition of e it follows that $o(l \bmod p^s) = e$.

(4). *$e = 2, 3, 4$ or 6, and p is odd.* Assume that $\varphi(e) \ge 3$. Then there exists i such that $1 < i < e-1$ and $(i, e) = 1$. We may write $g = g_1 g_2$ such that $(o(g_1), i) = 1$ and each prime factor of $o(g_2)$ divides i. Then $o(g_1) = o(g_1^i)$ and $(o(g_1), o(g_2)) = 1$. Also, since $(i, e) = 1$, we have $(o(g_2), e) = 1$. Since $g_1^e g_2^e = g^e \in \mathbf{C}_{\langle z\rangle}(M_p)$, also $g_2^{eo(g_1^e)} = g^{eo(g_1^e)} \in \mathbf{C}_{\langle z\rangle}(M_p)$. Further, since $(o(g_2), eo(g_1^e)) = 1$, there exists an integer k such that $eo(g_1^e)k \equiv 1 (\mathrm{mod}\, o(g_2))$. Therefore, $g_2 = g_2^{eo(g_1^e)k} \in \mathbf{C}_{\langle z\rangle}(M_p)$, and so $g_1^e = g^e g_2^{-e} \in \mathbf{C}_{\langle z\rangle}(M_p)$. Now $x^{g_1} = x^{g_1 g_2} = x^g = x^l$ for all $x \in M_p$. Since G is an FIF-group and $o(g_1) = o(g_1^i)$, there exists $\alpha \in \mathrm{Aut}(G)$ such that $g_1^\alpha = g_1^{\varepsilon i}$ for some $\varepsilon = \pm 1$. Since M_p is characteristic in G, we have $y := x^\alpha \in M_p$ with $o(y) = o(x)$. Therefore,

$$g_1^{-\varepsilon i} y g_1^{\varepsilon i} = (g_1^{-1} x g_1)^\alpha = (x^l)^\alpha = y^l = g_1^{-1} y g_1,$$

that is, $g_1^{-\varepsilon i+1} y g_1^{\varepsilon i-1} = y$. Consequently, $y^{l^{\varepsilon i-1}} = g_1^{-\varepsilon i+1} y g_1^{\varepsilon i-1} = y$, and hence, taking $x \in M_p$ with $o(x) = p^s$ so that $o(y) = p^s$, we have $l^{\varepsilon i-1} \equiv 1 (\mathrm{mod}\, p^s)$. Therefore, if $\varepsilon = 1$, then e divides $i-1$; if $\varepsilon = -1$, then e divides $i+1$, either of which is contrary to $1 < i < e-1$. Hence $\varphi(e) \le 2$ and so $e = 2, 3, 4$ or 6.

Since $\langle a\rangle^g = \langle a\rangle$ and $a^g = a^l \ne a$, g induces a nontrivial automorphism of $\langle a\rangle$. If $p = 2$ then $\mathrm{Aut}(\langle a\rangle)$ is a 2-group. Thus g is of even order, a contradiction. Therefore, $p \ge 3$. Hence part (ii) holds. □

The next result characterises a special subclass of the 2-CI-groups occurring in Theorem 4.2 (1).

PROPOSITION 4.4. *Suppose that $G = M \rtimes \langle z \rangle$ is a 2-CI-group, where*

(i) *M is abelian and each Sylow subgroup is homocyclic;*
(ii) *$(|M|, o(z)) = 1$, z normalizes each cyclic subgroup of M of prime-power order; and*
(iii) *G is not nilpotent and is coprime-indecomposable.*

Then $G = H_e(M, 2^r 3^s, l)$, where l has order e modulo $\exp(M)$ and e, r, s are as in Table 1.

PROOF. Let n be the exponent of M. First we prove that there exist integers $e \in \{2, 3, 4, 6\}$, and l of order e modulo n, such that $x^z = x^l$ for all $x \in M$. Since M is nilpotent, $M = M_1 \times \cdots \times M_t$ where $M_i = \mathbb{Z}_{p_i^{s_i}}^{d_i}$ is the Sylow p_i-subgroup of M and $p_1, \ldots, p_t$ are the distinct prime divisors of $|M|$. Note that $n = \prod p_i^{s_i}$. Choose $i \leq t$. Since G is coprime-indecomposable, z does not centralize M_i. Hence, by Lemma 4.3, there exist integers l_i and e_i such that $e_i \in \{2, 3, 4, 6\}$, l_i has order e_i modulo $p_i^{d_i}$ and $x^z = x^{l_i}$ for all $x \in M_i$. By the Chinese Remainder Theorem (see [19, p. 64]), there is an integer l such that $1 \leq l < n$ and for all i, $l \equiv l_i \pmod{p_i^{s_i}}$. Each $x \in M$ has a unique expression as $x = x_1 \ldots x_t$ with $x_i \in M_i$, and we have, therefore, $x^z = x_1^z \ldots x_t^z = x_1^{l_1} \ldots x_t^{l_t} = x_1^l \ldots x_t^l = x^l$ for all $x \in M$. Let $e = lcm\{e_1, \ldots, e_t\}$, so $e \in \{2, 3, 4, 6, 12\}$. Since $o(l_i \bmod p^{s_i}) = e_i$ for all i, also $o(l \bmod p^{s_i}) = e_i$ for all i, and hence $o(l \bmod n) = e$. Suppose that for some prime q dividing $o(z)$, a Sylow q-subgroup $\langle z_q \rangle$ of $\langle z \rangle$ centralizes M. Then $G = M \rtimes (\langle z_{q'} \rangle \times \langle z_q \rangle) = (M \rtimes \langle z_{q'} \rangle) \times \langle z_q \rangle$, where $\langle z_{q'} \rangle$ is the Hall q'-subgroup of $\langle z \rangle$. This is a contradiction since G is coprime-indecomposable. Hence no nontrivial Sylow subgroup of $\langle z \rangle$ centralizes M. In particular, since z^e centralizes M and e divides 12, we must have $o(z) = 2^r 3^s$ for some integers r and s. Suppose that $e = 12$. Since G is a 2-CI-group and $o(z) = o(z^5)$, there exists $\alpha \in \mathrm{Aut}(G)$ such that $z^\alpha = z^{5\varepsilon}$ for some $\varepsilon = \pm 1$. As M is characteristic in G, there exists $u := x^\alpha \in M$ with $o(u) = n$, and so

$$z^{-5\varepsilon} u z^{5\varepsilon} = (z^{-1} x z)^\alpha = (x^l)^\alpha = u^l = z^{-1} u z,$$

that is, $z^{-5\varepsilon+1} u z^{5\varepsilon-1} = u$. Thus $u^{l^{5\varepsilon-1}} = z^{-5\varepsilon+1} u z^{5\varepsilon-1} = u$, and hence $l^{5\varepsilon-1} \equiv 1 \pmod{n}$. Hence $5\varepsilon - 1$ is divisible by $e = 12$, which is not possible. Thus $e = 2, 3, 4$ or 6. Note that e divides $o(z)$. Thus if $r = 0$, then $e = e_1 = \cdots = e_t = 3$, and if $s = 0$, then each e_i is 2 or 4, so e is 2 or 4. Suppose that $r > 0$ and $s > 0$. If all the e_i are 2 or 4, then a Sylow 3-subgroup $\langle z_3 \rangle$ of $\langle z \rangle$ is nontrivial and centralizes M which is not the case. Hence, at least one of the e_i is equal to 3. Similarly at least one of the e_i is even, and hence $e = 6$. It now follows that $G = H_e(M, 2^r 3^s, l)$ and r, s, e are as in Table 1. □

Finally, we investigate another special subclass of 2-CI-groups satisfying Theorem 4.2 (1).

LEMMA 4.5. *Suppose that G is a 2-CI-group which is coprime-indecomposable and not nilpotent. Suppose further that G satisfies Theorem 4.2 (1) and that $G = M \rtimes \langle z \rangle$ with $(|M|, o(z)) = 1$ and $M = \mathbb{Z}_2^2$ or Q_8. Then $\langle z \rangle$ is a 3-group and acts nontrivially on M.*

PROOF. Since $(|M|, o(z)) = 1$, $o(z)$ is odd. Also $G/(\mathbf{C}_G(M)M) \leq \mathrm{Out}(M) \cong \mathrm{S}_3$, and since $o(z)$ is odd, we have that $|G/\mathbf{C}_G(M)M| = 1$ or 3. If there is a prime q dividing $o(z)$ such that q does not divide $|G/\mathbf{C}_G(M)M|$, then a Sylow q-subgroup $\langle z_q \rangle$ of $\langle z \rangle$ centralizes M. Thus $G = M \rtimes (\langle z_{q'} \rangle \times \langle z_q \rangle) = (M \rtimes \langle z_{q'} \rangle) \times \langle z_q \rangle$ where $\langle z_{q'} \rangle$ is a Hall q'-subgroup of $\langle z \rangle$, which is a contradiction since G is coprime-indecomposable. Since G is coprime-indecomposable and not nilpotent, we have that $|G/\mathbf{C}_G(M)M| = 3$, and so $\langle z \rangle$ is a 3-group. □

5. Structure of Certain 4-CI-groups

In this section we prove several technical lemmas concerning 4-CI-groups, which will be applied to prove Theorem 1.1 in the next section. Recall that the *direct product* $\Gamma_1 \times \Gamma_2$ of two graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ is the graph with vertex set $V_1 \times V_2$ such that (u_1, u_2) is adjacent to (v_1, v_2) if and only if either $\{u_1, v_1\} \in E_1$ and $u_2 = v_2$, or $\{u_2, v_2\} \in E_2$ and $u_1 = v_1$. The first lemma analyses the groups listed in Theorem 4.2 (1). It will also be used to assist our analysis of the groups in Theorem 4.2 (2).

Proposition 5.1. *Suppose that $G = M \rtimes \langle z \rangle$ is a 4-CI-group satisfying Theorem* 4.2 (1), *where*

(i) *M has a homocyclic Sylow p-subgroup M_p for some prime p dividing $|M|$;*
(ii) *$(|M|, o(z)) = 1$, and $\langle z \rangle$ has a Sylow q-subgroup $G_q = \langle h \rangle$ for some prime q dividing $o(z)$ such that there is a cyclic subgroup $\langle a_0 \rangle$ of M_p which is not normalized by h;*
(iii) *G is coprime-indecomposable.*

Then $p = 2$, $q = 3$, $M_p = \mathbb{Z}_2^2$, and h^3 centralizes M_p.

Proof. Now $M_p = \mathbb{Z}_{p^t}^d$ for some $t \geq 1$, and we must have $d \geq 2$ since G_q does not normalize $\langle a_0 \rangle$. Set $K := M \rtimes G_q$. Since G_q is characteristic in $\langle z \rangle$, it follows that K is characteristic in G, and so K is also a 4-CI-group (see Lemma 2.1). Since G_q does not normalize $\langle a_0 \rangle$, by Lemma 4.3, $\langle a \rangle \cap \langle a^h \rangle = 1$ for all $a \in M_p$. Let g be an element of G_q with minimal order such that $\langle a \rangle \cap \langle a^g \rangle = 1$ for all $a \in M_p$. Then $\langle a \rangle \cap \langle a^{g^q} \rangle \neq 1$ for some $a \in M_p$. By Lemma 4.3, g^q normalizes every cyclic subgroup of M_p.

Let $\mathrm{Sub}(p^t)$ be the set of all cyclic subgroups of M_p of order p^t. We claim that G_q acts transitively on $\mathrm{Sub}(p^t)$ by conjugation. Take $\langle a \rangle \in \mathrm{Sub}(p^t)$ and let $b = a^g$. Then $\langle a \rangle \cap \langle b \rangle = 1$, and thus, for any $\langle x \rangle \in \mathrm{Sub}(p^t)$, either $\langle x \rangle \cap \langle a \rangle = 1$ or $\langle x \rangle \cap \langle b \rangle = 1$. Assume first that $\langle x \rangle \cap \langle a \rangle = 1$, and let $S = \{a, a^{-1}, b, b^{-1}\}$ and $T = \{a, a^{-1}, x, x^{-1}\}$. Then $\mathrm{Cay}(\langle S \rangle, S) \cong C_{p^t} \times C_{p^t} \cong \mathrm{Cay}(\langle T \rangle, T)$, and so $\mathrm{Cay}(K, S) \cong \mathrm{Cay}(K, T)$ (by Lemma 2.1). Since K is a 4-CI-group, there exists $\alpha \in \mathrm{Aut}(K)$ such that $S^\alpha = T$. Hence $(\langle a \rangle, \langle b \rangle)^\alpha = (\langle a \rangle, \langle x \rangle)$ or $(\langle x \rangle, \langle a \rangle)$. Note that, since $g^{-1}ag = b$,

$$(g^\alpha)^{-1} \langle a \rangle^\alpha g^\alpha = \langle g^{-1}ag \rangle^\alpha = \langle b \rangle^\alpha.$$

Thus in the first case $(g^\alpha)^{-1} \langle a \rangle g^\alpha = \langle x \rangle$, while in the second case $(g^\alpha)^{-1} \langle x \rangle g^\alpha = \langle b \rangle^\alpha = \langle a \rangle$. Now $g^\alpha = cg^i$ for some $c \in M$ and some integer i, and since c centralizes M_p, we have either $g^{-i} \langle a \rangle g^i = \langle x \rangle$ or $g^{-i} \langle x \rangle g^i = \langle a \rangle$. Thus in either case, $\langle x \rangle$ is conjugate to $\langle a \rangle$ by some element of $\langle g \rangle$. If $\langle x \rangle \cap \langle b \rangle = 1$, then similarly $\langle x \rangle$ is conjugate to $\langle b \rangle$ by some element of $\langle g \rangle$. Consequently, since $\langle a \rangle^g = \langle b \rangle$, in this case also $\langle x \rangle$ is conjugate to $\langle a \rangle$ by some element of $\langle g \rangle$. Thus $\langle g \rangle$ is transitive on $\mathrm{Sub}(p^t)$ by conjugation. Since $G_q \geq \langle g \rangle$, G_q also acts transitively on $\mathrm{Sub}(p^t)$, and since G_q is abelian, G_q induces a regular permutation group on $\mathrm{Sub}(p^t)$ (see [25, Proposition 4.4]). Let E be the kernel of this G_q-action. Then $|G_q : E| = |\mathrm{Sub}(p^t)| = s$, say, and $E = \langle h^s \rangle$. Since $\langle g \rangle$ is transitive on $\mathrm{Sub}(p^t)$, it follows that $G_q = \langle g \rangle$, and since g^q normalizes every cyclic subgroup of M_p, we have $E = \langle g^q \rangle = \langle h^q \rangle$ and $q = |\mathrm{Sub}(p^t)|$. Therefore,

$$q = |\mathrm{Sub}(p^t)| = \frac{p^{td} - p^{(t-1)d}}{\varphi(p^t)} = p^{(t-1)(d-1)} \frac{p^d - 1}{p - 1}.$$

Since q is a prime and $d \geq 2$, it follows that $p^{(t-1)(d-1)} = 1$, and so $t = 1$, $M_p \cong \mathbb{Z}_p^d$ and $q = \frac{p^d - 1}{p-1}$. In particular $q \geq 3$, and since $\frac{p^d-1}{p-1}$ is prime, d must also be a prime. If $q = 3$, then $p^d = 2^2$ and so h^q centralizes $M_p \cong \mathbb{Z}_2^2$ and the lemma holds.

Thus we may suppose that $q \geq 5$ and hence that d is an odd prime. Since g^q normalizes every cyclic subgroup of M_p, by Lemma 4.3 (ii), $(h^q)^e \in \mathbf{C}_{G_q}(M_p)$ where $e \in \{2, 3, 4, 6\}$, and so also h^q centralizes M_p. Let $C_{p'}$ be a Hall p'-subgroup of $C := \mathbf{C}_K(M_p)$. Then $C = M_p \times C_{p'}$ and hence we have $C_{p'}$ *char* C *char* K. By Lemma 2.2, the 4-CI-group K is an FIF-group. Thus, by Lemma 2.3 (i), $\overline{K} := K/C_{p'}$ is an FIF-group. Since $h^q \in \mathbf{C}_K(M_p)$, we have $\overline{K} = \overline{M}_p \rtimes \langle \overline{h} \rangle$, where $\overline{M}_p = M_p C_{p'}/C_{p'} \cong \mathbb{Z}_p^d$ and $\langle \overline{h} \rangle = \langle h \rangle C_{p'}/C_{p'} \cong \langle h \rangle / \langle h^q \rangle \cong \mathbb{Z}_q$. Since $\overline{K}$ is an FIF-group, it follows that all cyclic subgroups of $\overline{K}$ of order p are conjugate under $\mathrm{Aut}(\overline{K})$, and so $\overline{M}_p$ is a minimal characteristic subgroup of $\overline{K}$. Further, h does not centralize M_p, and hence $\mathbf{C}_{\overline{K}}(\overline{M}_p) = \overline{M}_p$. So $\overline{K}$ satisfies all the conditions of Lemma 2.3 (ii), and hence $\frac{1}{2}\varphi(q)$ divides d. On the other hand, $\varphi(q) = q - 1 = \frac{p^d-1}{p-1} - 1 = \frac{p^d-p}{p-1}$, so $\frac{p^d-p}{2p-2}$ divides d. The only possibility for (p, d, q) satisfying this divisibility condition (with $q \geq 5$ and d an odd prime) is $(2, 3, 7)$. Thus $M_p \cong \mathbb{Z}_2^3$, and we may write $M_p \setminus \{1\} = \{a_0, a_1, \ldots, a_6\}$ such that $a_i^h = a_{i+1}$ (reading the subscripts modulo 7). Let $S = \{a_0, a_1, a_2\}$. Then it is easy to check that $\langle S \rangle = M_p$. Since $a_0, a_1, \ldots, a_6$ are distinct and $\langle a_0, a_1 \rangle$ contains exactly three involutions (namely, a_0, a_1 and a_0a_1), there exists $k \in \{3, 5\}$ satisfying $a_k \notin \langle a_0, a_1 \rangle$ so that $\langle a_0, a_1, a_k \rangle = M_p$. Let $T = \{a_0, a_1, a_k\}$. Then $\mathrm{Cay}(M_p, S) \cong \mathbf{Q}_3 \cong \mathrm{Cay}(M_p, T)$ where $\mathbf{Q}_3$ is the cube graph of dimension 3, so $\mathrm{Cay}(K, S) \cong \mathrm{Cay}(K, T)$ (see Lemma 2.1). Since K is a 4-CI-group, $S^\alpha = T$ for some $\alpha \in \mathrm{Aut}(K)$. Thus $a_0^\alpha = a_i$ for some $i \in \{0, 1, k\}$ and $h^\alpha = ch^j$ for some $c \in M$ and some integer $j \geq 1$. Consequently, noting that c centralizes M_p, $a_1^\alpha = (h^{-1}a_0h)^\alpha = h^{-j}a_ih^j = a_{i+j}$ and $a_2^\alpha = (h^{-1}a_1h)^\alpha = h^{-j}a_{i+j}h^j = a_{i+2j}$. Thus $\{i, i + j, i + 2j\} \equiv \{0, 1, k\} (\mathrm{mod}\, 7)$. However, it is straightforward to check that there are no values of i, j for which this holds, for $k = 3$ or $k = 5$. This completes the proof. □

Now we consider the groups listed in Theorem 4.2 (2).

PROPOSITION 5.2. *Suppose that G is a 4-CI-group which is coprime-indecomposable. Suppose further that G satisfies Theorem* 4.2 (2). *Then $G = \mathbb{Z}_3^2 \rtimes \mathrm{Q}_8$.*

PROOF. We use the notation of Theorem 4.2 so that $G = (L \times M) \rtimes ((H \rtimes K) \times \mathbb{Z}_n)$, every Sylow subgroup of $L \times M$ is homocyclic, $\langle M, H \rangle = M \times H$, $\langle L, \mathbb{Z}_n \rangle = L \times \mathbb{Z}_n$ and either H is cyclic or $H = \mathrm{Q}_8$. It follows, since $\langle M, H \rangle = M \times H$, that $L \rtimes H$ is a characteristic subgroup of G, and so by Lemma 2.1, $L \rtimes H$ is also a 4-CI-group.

Suppose that H is cyclic. By Theorem 4.2, H is of odd order, and either $|L|$ is odd or a Sylow 2-subgroup of L is $\mathbb{Z}_2^3$. It follows from Proposition 5.1 that each Sylow subgroup of H normalizes each cyclic subgroup of L of prime-power order. Moreover, by Theorem 4.2, $L \rtimes H$ is not nilpotent and is either coprime-indecomposable, or is the direct product of two non-nilpotent coprime indecomposable factors. Each coprime indecomposable factor satisfies the hypotheses of Proposition 4.4. Since $|H|$ is odd, it follows from Proposition 4.4 that $L \rtimes H$ is coprime-indecomposable and $L \rtimes H = H_3(L, 3^t, l)$ for some positive integers t and l, and in particular, $H = \langle y \rangle = \mathbb{Z}_{3^t}$ and H centralizes no nontrivial Sylow subgroup of L. It follows that L, $H \rtimes K$ are as in line 2 of the table in Theorem 4.2. Thus $K = \langle z \rangle \cong \mathbb{Z}_{2^r}$ and $L = (\mathbb{Z}_{5^{u_1}7^{u_2}11^{u_3}})^2$. Let L_p be a nontrivial Sylow p-subgroup of L. Then $soc(L_p) = \mathbb{Z}_p^2$ and the conjugation action induces a homomorphism φ from $H \rtimes K$ to $\mathrm{Aut}(soc(L_p)) = \mathrm{GL}_2(p)$. Since $\varphi(H) \neq 1$ and H normalizes each cyclic subgroup of $soc(L_p)$, it follows that $\varphi(H) \cong \mathbb{Z}_3$ consists of scalar matrices, so $p = 7$. Since $\varphi(H)$ is central in $\varphi(H \rtimes K)$ but K does not centralize H, it follows that $y^z = y^{1+3j}$ for some j such that $1 \leq j < 3^{t-1}$, and $j \not\equiv 0 (\mathrm{mod}\, 3)$. However this means that $o(z)$ is divisible by 3, which is a contradiction.

Therefore, by Theorem 4.2, $H = \mathrm{Q}_8$, $K = \mathbb{Z}_{3^s}$, $L = \mathbb{Z}_q^2$, and $F := L \rtimes H = \mathbb{Z}_q^2 \rtimes \mathrm{Q}_8$ is a 4-CI-group. Let $H = \langle x, y \rangle$. Then $L \rtimes \langle x^2 \rangle$ *char* $L \rtimes H$, and it follows that $L \rtimes \langle x^2 \rangle$ is

also a 4-CI-group. It follows from Lemma 4.3 that the involution x^2 normalizes every cyclic subgroup of L of prime-power order. For each prime p dividing q, let $L_p \equiv \mathbb{Z}_{p^t}^2$ denote the Sylow p-subgroup of L. Suppose that x^2 centralizes L_p for some p. Let $L_{p'}$ be a Hall p'-subgroup of L. Then $L_{p'}$ *char* L *char* F and $F/L_{p'} \cong L_p \rtimes Q_8$. By Lemma 2.3, $F/L_{p'}$ is an FIF-group. Since x^2 centralizes L_p, again by Lemma 2.3, $F/(L_{p'}.\langle x^2\rangle) \cong L_p \rtimes \mathbb{Z}_2^2$ is an FIF-group. By [16, Theorem 1.1], it follows that this group is ismorphic to $L_p \times \mathbb{Z}_2^2$ and hence H centralizes L_p, which is a contradiction to Theorem 4.2(2)(ii) (that is, a contradiction to the fact that H centralizes no Sylow subgroup of L). Therefore, x^2 does not centralize L_p for any p, and it follows from Lemma 4.3 that x^2 inverts every element of L_p for all p and, hence, x^2 inverts every element of L. Now let $L_p = \mathbb{Z}_{p^t}^2$ and let $a \in L_p$ of order p^t. Since $\mathbf{N}_F(\langle a^{p^{t-1}}\rangle)/\mathbf{C}_F(\langle a^{p^{t-1}}\rangle)$ is cyclic and $\mathbf{C}_F(\langle a^{p^{t-1}}\rangle) \cap H = 1$, at least one of x and y does not normalize $\langle a^{p^{t-1}}\rangle$, x say. Thus $\langle (a^{p^{t-1}})^x\rangle \cap \langle a^{p^{t-1}}\rangle = 1$ and since $\langle a^{p^{t-1}}\rangle$ is the unique subgroup of $\langle a\rangle$ of order p, $\langle a^x\rangle \cap \langle a\rangle = 1$. Let $b = a^x$. Then for any $c \in L_p$ with $o(c) = p^t$, either $\langle c\rangle \cap \langle a\rangle = 1$, or $\langle c\rangle \cap \langle b\rangle = 1$, say $\langle c\rangle \cap \langle a\rangle = 1$.

Set $S := \{a, a^{-1}, b, b^{-1}\}$ and $T := \{a, a^{-1}, c, c^{-1}\}$. Now $\mathrm{Cay}(\langle S\rangle, S) \cong C_{p^t} \times C_{p^t} \cong \mathrm{Cay}(\langle T\rangle, T)$, and thus $\mathrm{Cay}(F, S) \cong \mathrm{Cay}(F, T)$ (see Lemma 2.1). Since F is a 4-CI-group, S is conjugate to T under $\mathrm{Aut}(F)$. Consequently, there exists $\alpha \in \mathrm{Aut}(F)$ such that $\{\langle a\rangle, \langle b\rangle\}^\alpha = \{\langle a\rangle, \langle c\rangle\}$. Since $x^{-1}\langle a\rangle x = \langle b\rangle$, we have that $(x^\alpha)^{-1}\langle a\rangle^\alpha x^\alpha = \langle b\rangle^\alpha$. It follows that $\langle a\rangle$ is conjugate to $\langle c\rangle$ by x^α or $(x^\alpha)^{-1}$. Now $x^\alpha = dx'$ for some $d \in L$ and some $x' \in H$. Since d centralizes L, $\langle a\rangle$ is conjugate to $\langle c\rangle$ by x' or $(x')^{-1}$. It follows that H acts transitively by conjugation on the set Ω of all subgroups of L_p of order p^t, and the kernel of this action contains $\langle x^2\rangle$ (since x^2 inverts each element of L_p). Hence $|\Omega|$ divides 4 and it follows that $p^t = 3$. Thus $L = L_p = \mathbb{Z}_3^2$, and by Theorem 4.2 (2), $M = 1$, $K = 1$ and $n = 1$. Thus $G = L \rtimes H = \mathbb{Z}_3^2 \rtimes Q_8$. □

6. Proof of Theorem 1.1

Let G be an m-CI-group for some $m \geq 4$. Then G is a 2-CI-group, so G is one of the groups listed in Theorem 4.2. Thus $G = X_1 \times \cdots \times X_l$ such that $(|X_i|, |X_j|) = 1$ and each X_i is coprime-indecomposable and satisfies part (1), (2) or (3) of Theorem 4.2. Since X_i *char* G, X_i is an m-CI-group (see Lemma 2.1). If X_i is nilpotent then X_i is a Sylow subgroup of G, and so either X_i is homocyclic, or $X_i \cong Q_8$. Thus, if $X_1, \ldots, X_l$ are all nilpotent, then the theorem holds, so we may assume that this is not the case. Note that the direct product U of all the nilpotent groups X_i (if any) is abelian. Suppose now that $X = X_i$ is not nilpotent. We shall prove that X is one of the non-nilpotent groups listed in parts (i)–(iii) of Theorem 1.1.

If X satisfies Theorem 4.2 (2) then by Proposition 5.2, $X \cong \mathbb{Z}_3^2 \rtimes Q_8$, as in part (i). Suppose next that X satisfies Theorem 4.2 (3), that is, $X = L_2(5)$, $L_2(8)$, $SL_2(5)$, $SL_2(7)$ or $SL_2(9)$. Since, by Lemma 3.1, a Sylow 2-subgroup of X is elementary abelian, cyclic or Q_8, it follows that X is one of $L_2(5) \cong A_5$, $L_2(8)$ or $SL_2(5)$. However, by Theorem 4.1, $L_2(8)$ is not a 3-CI-group. Thus $X = A_5$ or $SL_2(5)$, as in part (i).

Finally, suppose that X satisfies Theorem 4.2 (1), that is, $X = M \rtimes \langle z\rangle$ where M is nilpotent and $(|M|, n) = 1$. First assume that a Sylow 2-subgroup M_2 of M is neither $\mathbb{Z}_2^2$ nor Q_8. Then every Sylow subgroup of M is homocyclic and is not isomorphic to $\mathbb{Z}_2^2$, and by Proposition 5.1, z normalizes every cyclic subgroup of M of prime-power order. Further, since X is coprime-indecomposable, no nontrivial Sylow subgroup of $\langle z\rangle$ centralizes M. Then by Proposition 4.4, $X = H_e(M, 2^r 3^s, l)$ where l has order e modulo $\exp(M)$, and r, s, e are as in one of the lines of Table 1, as in part (iii).

Now assume that a Sylow 2-subgroup M_2 of M is isomorphic to $\mathbb{Z}_2^2$ or Q_8. Then n is odd. Let $M_{2'}$ be the Hall $2'$-subgroup of M. Then $M_{2'}$ is a characteristic abelian subgroup of X and $M = M_2 \times M_{2'}$. Note that $\mathrm{Out}(M_2) \cong S_3$. It follows, since n is odd, that $X/\mathbf{C}_X(M_2)M_2 \leq \mathbb{Z}_3$. Suppose that there is a Sylow p-subgroup M_p of M, and a Sylow q-subgroup $\langle z_q \rangle$ of $\langle z \rangle$, for some odd primes p and q, such that z_q does not centralize M_p. It follows from Proposition 5.1 that z_q normalizes every cyclic subgroup of M_p and then by Lemma 4.3 (noting that q is odd) that $q = 3$, and $x^{z_q} = x^l$ for all $x \in M_p$, where l has order 3 modulo the exponent of M_p.

Thus, if there is a prime $q > 3$ such that q divides $o(z)$, then the Sylow q-subgroup $\langle z_q \rangle$ of $\langle z \rangle$ centralizes $M_{2'}$. However, z_q also centralizes M_2, and it follows that $\langle z_q \rangle$ is a direct factor of X contradicting the fact that X is coprime-indecomposable. Hence $\langle z \rangle \cong \mathbb{Z}_{3^s}$ for some $s \geq 1$. Again, since X is coprime-indecomposable, z does not centralize M_2, and if p is an odd prime dividing $|M|$ then z does not centralize the Sylow p-subgroup M_p. Suppose now that $M \neq M_2$ so that such an odd prime p exists and (by the previous paragraph) $x^z = x^l$ for all $x \in M_p$, where l has order 3 modulo the exponent of M_p. Note that l has order 3 modulo p, so $p \equiv 1 \pmod 3$ and, in particular, $p \geq 7$.

Let a_0, a_1 be distinct elements of M_2 such that $a_0^z = a_1$ and let b be an element of M_p of order p. Then $b^z = b^l$. Set $S = \{a_0 b^l, (a_0 b^l)^{-1}, a_1 b, (a_1 b)^{-1}\}$ and $T = \{a_0 b, (a_0 b)^{-1}, a_1 b^l, (a_1 b^l)^{-1}\}$. Then $\langle S \rangle = \langle T \rangle = M_2 \times \langle b \rangle$ and there exists an automorphism σ of $\langle S \rangle$ such that $(a_1 b)^\sigma = a_0 b$ and $(a_0 b^l)^\sigma = a_1 b^l$. Thus $\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\langle T \rangle, T)$ and so $\mathrm{Cay}(X, S) \cong \mathrm{Cay}(X, T)$ (by Lemma 2.1). Since X is a 4-CI-group, there is an element $\rho \in \mathrm{Aut}(X)$ such that $S^\rho = T$. Thus $(a_0 b^l, a_1 b)^\rho = ((a_0 b)^\varepsilon, (a_1 b^l)^{\varepsilon'})$ or $((a_1 b^l)^{\varepsilon'}, (a_0 b)^\varepsilon)$, where $\varepsilon, \varepsilon' = \pm 1$. Since $(o(b), o(a_i)) = 1$, it follows that either

$$(a_0, a_1)^\rho = (a_0^\varepsilon, a_1^{\varepsilon'}) \text{ and } (b^l, b)^\rho = (b^\varepsilon, b^{l\varepsilon'}), \text{ or}$$
$$(a_0, a_1)^\rho = (a_1^{\varepsilon'}, a_0^\varepsilon) \text{ and } (b^l, b)^\rho = (b^{l\varepsilon'}, b^\varepsilon).$$

Since l has order 3 modulo the exponent of M_p, and $p \geq 7$ it follows that l has order 3 modulo p and in particular $l^2 \not\equiv \pm 1 \pmod p$. Suppose that the first line above holds. Then $b^\rho = b^{l\varepsilon'}$, and $b^\varepsilon = (b^l)^\rho = (b^\rho)^l = b^{l^2\varepsilon'}$ which implies that $p = o(b)$ divides $l^2 \pm 1$, which is a contradiction. Hence the second line holds, so $b^\rho = b^\varepsilon$ and $b^{l\varepsilon'} = (b^l)^\rho = (b^\rho)^l = b^{\varepsilon l}$. This means that p divides $l(\varepsilon' - \varepsilon)$ whence $\varepsilon' = \varepsilon$. Now $z^\rho = cz^i$ for some $c \in M$ and some integer i, where $1 \leq i < 3^s$ and $i \equiv \pm 1 \pmod 3$. Note that $b^c = b$. Thus we have

$$b^{l\varepsilon} = (b^l)^\rho = (z^{-1}bz)^\rho = z^{-i}c^{-1}b^\varepsilon cz^i = z^{-i}b^\varepsilon z^i = b^{\varepsilon l^i}$$

whence $l^{i-1} \equiv 1 \pmod p$. Since $l^3 \equiv 1 \pmod p$ it follows that $i \equiv 1 \pmod 3$. On the other hand, since $z^{-1}a_0 z = a_1$ and z^3 centralizes M_2, we have that

$$z^{-1}a_1^\varepsilon z = z^{-i}a_1^\varepsilon z^i = (z^{-1}a_0 z)^\rho = a_1^\rho = a_0^\varepsilon.$$

Thus $z^{-2}a_1 z^2 = z^{-1}a_0 z = a_1$, that is z^2 centralizes a_1, and similarly, z^2 centralizes a_0. So z^2 centralizes $M_2 = \langle a_0, a_1 \rangle$, which is a contradiction. Therefore, $M_{2'} = 1$ and so $X = M_2 \rtimes \mathbb{Z}_{3^s} = \mathbb{Z}_2^2 \rtimes \mathbb{Z}_{3^s}$ or $Q_8 \rtimes \mathbb{Z}_{3^s}$, as in part (ii).

Thus each of the non-nilpotent X_i is one of the groups listed in parts (i)–(iii) of Theorem 1.1. If there is only one non-nilpotent X_i then the theorem holds, so suppose that two of the X_i are not nilpotent, say X_1 and X_2. Since the $|X_i|$ are relatively prime, and since each of the groups in parts (i)–(iii) has order divisible by 2 or 3, there are only two such groups X_i; one of them is $H_3(M', 3^s, l')$ and the other has even order relatively prime to 3 and so is Q_8 or $H_e(M, 2^r, l)$ with $e = 2$ or 4. This completes the proof of the theorem. □

ACKNOWLEDGEMENTS

The first author gratefully acknowledges the support of an Overseas Postgraduate Research Scholarship of the Australian Department of Education, Employment and Training and a University Postgraduate Award from the University of Western Australia. This research forms part of an Australian Research Council small grant project.

REFERENCES

1. A. Adám, Research problem 2-10, *J. Comb. Theory*, **2** (1967), 309.
2. B. Alspach and T. D. Parsons, Isomorphisms of circulant graphs and digraphs, *Discrete Math.*, **25** (1979), 97–108.
3. L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hung.*, **29** (1977), 329–336.
4. L. Babai and P. Frankl, Isomorphisms of Cayley graphs I, *Colloq. Math. Soc. J. Bolyai*, **18***; Combinatorics, Keszthely*, 1976; North-Holland, Amsterdam, 1978, pp. 35–52.
5. L. Babai and P. Frankl, Isomorphisms of Cayley graphs II, *Acta Math. Acad. Sci. Hung.*, **34** (1979), 177–183.
6. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
7. C. Delorme, O. Favaron and M. Maheo, Isomorphisms of Cayley multigraphs of degree 4 on finite abelian groups, *Europ. J. Combinatorics*, **13** (1992), 59–61.
8. E. Dobson, Isomorphism problem for Cayley graph of $\mathbb{Z}_p^3$, *Discrete Math.*, **147** (1995), 87–94.
9. B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Comb. Theory*, **9** (1970), 297–307.
10. X. G. Fang and M. Y. Xu, On isomorphisms of Cayley graphs of small valency, *Algebra Colloq.*, **1** (1994), 67–76.
11. C. D. Godsil, On Cayley graphs isomorphisms, *Ars Comb.*, **15** (1983), 231–246.
12. C. H. Li, Isomorphisms and classification of Cayley graphs of small valencies on finite abelian groups, *Aust. J. Comb.*, **12** (1995), 3–14.
13. C. H. Li, On isomorphisms of connected Cayley graphs, *Discrete Math.*, **178**(1998), 109–122.
14. C. H. Li, Finite CI-groups are solvable, *Bull. London Math. Soc.* (to appear).
15. C. H. Li and C. E. Praeger, The finite simple groups with at most two fusion classes of every order, *Comm. Algebra*, **24** (1996), 3681–1704.
16. C. H. Li and C. E. Praeger, Finite groups in which any two elements of the same order are either fused or inverse-fused, *Comm. Algebra*, **25** (1997), 3081–3118.
17. C. H. Li, C. E. Praeger and M. Y. Xu, Finite groups with the Cayley isomorphism property, *J. Graph Theory*, **27** (1998), 21–31.
18. M. Muzychuk, Ádám's conjecture is true in the square-free case, *J. Comb. Theory Ser. A*, **72** (1995), 118–134.
19. I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, 1991.
20. L. A. Nowitz, A non-Cayley-invariant Cayley graph of the elementary abelian group of order 64, *Discrete Math.*, **110** (1992) 223–228.
21. P. P. Pàlfy, Isomorphism problem for relational structures with a cyclic automorphism, *Europ. J. Combinatorics*, **8** (1987), 35–43.
22. D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1982.
23. M. Suzuki, *Group Theory II*, Springer-Verlag, New York, 1982.
24. S. Toida, A note on Adám's conjecture, *J. Comb. Theory Ser. B*, **23** (1977), 239–246.
25. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

26. M. Y. Xu, Vertex-transitive graphs and finite simple groups, (unpublished manuscript), 1988.

Received 27 June 1997 and accepted 28 November 1998

C. H. Li and C. E. Praeger
Department of Mathematics and Statistics
The University of Western Australia
Nedlands, WA 6907
Australia